



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	10454-022001/P-4190-4	1821

52197 7590 02/23/2007
PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER

SHERR, CRISTINA O

ART UNIT	PAPER NUMBER
----------	--------------

3621

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/944,788

Applicant(s)

VALDES ET AL.

Examiner

Cristina Owen Sherr

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 November 2006.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,7,8,13,14,20,21,24,25,28 and 29 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _____ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's amendment filed November 20, 2006.

Election/Restrictions

2. Applicant's election without traverse of claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 in the reply filed on November 20, 2006 is acknowledged.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 2, 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nine et al (US 6,560,611).

7. Regarding claim 1 –

Nine discloses in an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

- (a) receiving a new alert (called "message" at col 3 ln 25-30);

Art Unit: 3621

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes(e.g. col 3 ln 12-20);

(c) updating a minimum similarity requirement for one or more features (e.g. col 5 ln 50-col 6 ln 10);

(d) updating a similarity expectation for one or more features (e.g. col 5 ln 50-col 6 ln 10);

(e) comparing the new alert with one or more alert classes, and either:

(f 1) associating the new alert with the existing alert class that the new alert most closely matches (col 7 ln 22-46); or

(f 2) defining a new alert class that is associated with the new alert (col 9 ln 5-22).

8. Although Nine discloses messages rather than “alerts”, the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

9. Regarding claim 2 –

Nine discloses the method of claim 1 further comprising the step (a) of passing each existing alert class through a transition model to generate a new prior belief state for each alert class (e.g. col 5 ln 60- col 6 ln 10).

10. As above, although Nine discloses messages rather than “alerts”, the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

Art Unit: 3621

11. Claims 7, 8, 13, 14, 20, 21, 24, 25, 28 and 29 are rejected under the same criteria as above.

12. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

13. Examiner acknowledges applicant's request for an examiner interview and deeply regrets that time constraints brought on by the hazardous weather conditions in the Washington, DC area during the week of February 11, 2007, made such an interview impossible. This examiner is normally open to examiner interview and quite flexible as to their scheduling. Should such an interview be desired at a future time, the examiner is more than willing to grant it.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cristina Owen Sherr whose telephone number is 571-272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.


Art Unit: 3621

15. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew J. Fischer can be reached on 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

16. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Cristina Owen Sherr
Patent Examiner, AU 3621



PIERRE EDDY ELISCA
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600